UNITED STATES DISTRICT COURT

for the

Western District of Washington

FILED LODGED
RECEIVED
November 2, 2020
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA
BY DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
SUJECT PERSON, SUBJECT PREMISES, and SUBJECT VEHICLE

Case No. MJ20-5254

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
The Subject Person, Subject Premises, and Subject Vechicle as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252 (a), (e)	Production of Child Pornography
Title 18, U.S.C. § 2252(a)(2), (b)(1)	Receipt/Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B), (b)(2)	Possession of Child Pornography (and Attempt/Conspiracy to commit these offenses)

The application is based on these facts:

✓ See attached Affidavit continued on the attached sheet

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

s/ Kelsey M. Mendoza
Applicant's signature

Special Agent Kelsey M. Mendoza, FBI
Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/02/2020

Judge's signature

City and state: Tacoma, Washington

David W. Christel, United States Magistrate Judge
Printed name and title

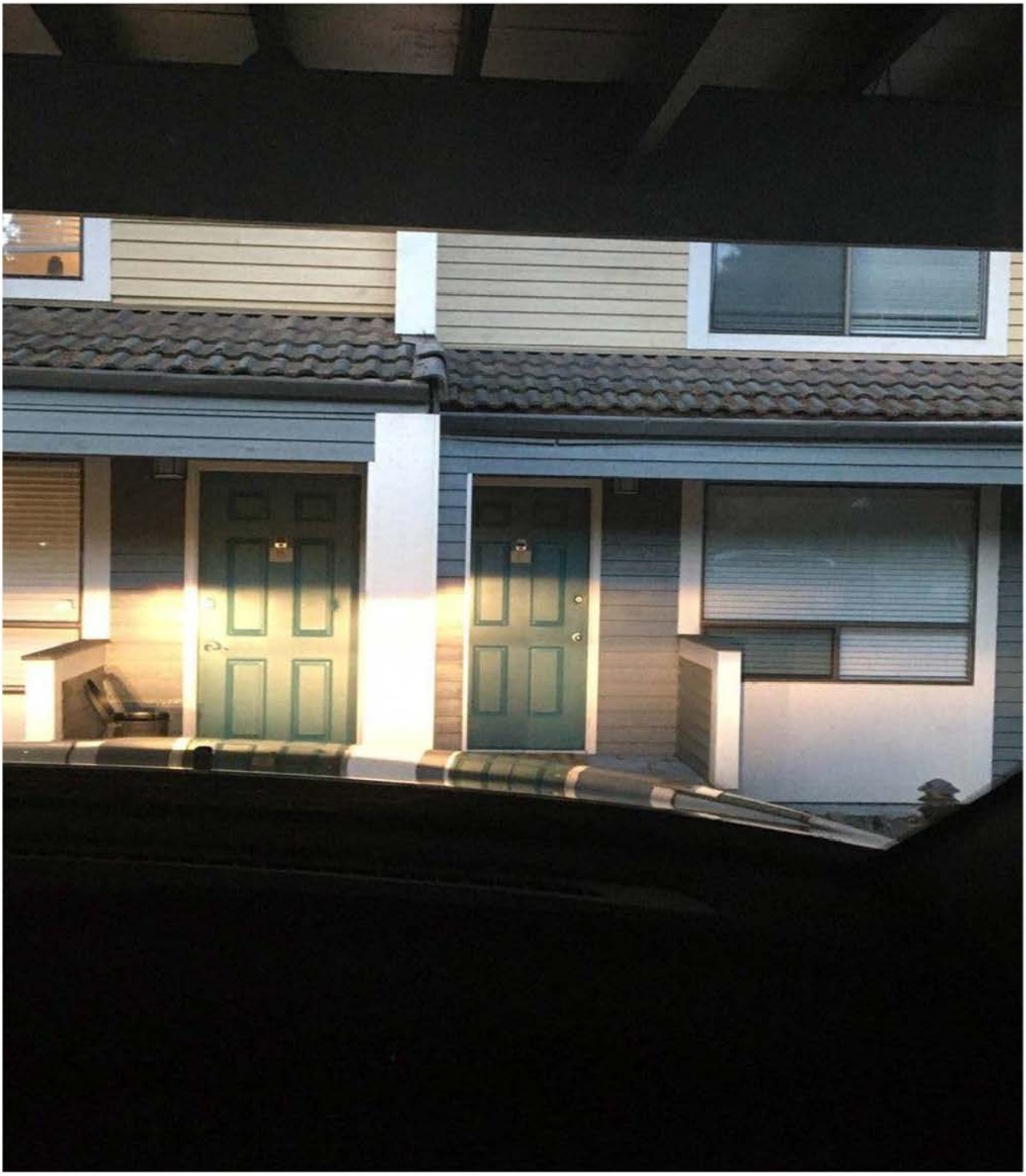
USAO #2020R01030

ATTACHMENT A

Description of Property to be Searched

The physical address of the SUBJECT PREMISES is 34 South 333rd Lane, Apt C, Federal Way, Washington 98003, which is described as Apartment C, a unit within a multiunit building. The pictures below depict the SUBJECT PREMISES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



The search is to include all rooms within Apartment C and any storage areas or parking/garage spaces exclusively assigned to Apartment C, as well as any digital

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

device(s) or other electronic storage media found therein. However, if law enforcement can reasonably determine onsite that the SUBJECT PERSON neither owns nor has access to a particular digital device or electronic storage medium, this warrant does not authorize its search or seizure.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The SUBJECT PERSON is MICHAEL MORRILL, YEAR OF BIRTH: 1972, SOCIAL SECURITY NUMBER: XXX-XX-2997.

The search shall include the SUBJECT PERSON and any backpacks, bags, or other containers that SUBJECT PERSON may be carrying, and any digital devices(s) or other electronic storage media found.

The SUBJECT VEHICLE is a 2019 Kia Forte (WA License BNK5436). The search shall include the entire SUBJECT VEHICLE and any digital devices(s) or other electronic storage media found

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography), as well as attempt or conspiracy to commit such offenses committed in or after July 2016, as follows:

a. Items, records, or information[7] relating to visual depictions of minors engaged in sexually explicit conduct;

b. Items, records, or information relating to the identity of the creator(s) of or subject(s) depicted in any visual depiction of a minor engaged in sexually explicit conduct;

c. Items, records, or information relating to the location of or circumstances surrounding the creation of any visual depiction of a minor engaged in sexually explicit conduct;

d. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

e. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

f. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;

---

[7] As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Items, records, or information related to communications with or about minors;

h. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;

i. Items, records, or information concerning travel;

j. Items, records, or information concerning websites operating over the Tor network, including any document or page comprising a part of any such website, records and information showing any person's access to or involvement with such websites, and any communications between any users of such websites;

k. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, purchase or lease agreements, diaries, statements, identification documents, address books, telephone directories, and keys;

l. Items, records, or information concerning the ownership or use of computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for internet access, handwritten notes, and computer manuals;

m. Any digital devices or other electronic storage media[8] and/or their components including:

i. any digital device or other electronic storage media capable of being used to commit, further, or store evidence, fruits, or instrumentalities of the offenses listed above;

[8] The term "digital devices" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "electronic storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ii. any magnetic, electronic or optical storage device capable of storing data, including thumb drives, SD cards, or external hard drives;

iii. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

iv. any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

n. For any digital device or other electronic storage media whose seizure is otherwise authorized by this warrant, and any digital device or other electronic storage media that contains or in which is stored records or information that is otherwise called for by this warrant:

i. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

vi. evidence of the times the digital device or other electronic storage media was used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

vii. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

viii. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

ix. records of or information about the Internet Protocol used by the digital device or other electronic storage media;

x. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

xi. contextual information necessary to understand the evidence described in this attachment.

o. A dark colored blanket with purplish-pink pattern and border.
p. A purple anal sexual object

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Kelsey M. Mendoza, being duly sworn on oath, depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since January 2019. I am currently assigned to the Seattle Division's Tacoma Resident Agency. As an FBI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, 2252A, 2422, and 2426. I have received specialized training from the FBI Academy consisting of legal classes, investigative techniques, evidence preservation and collection, financial related crimes, and other law enforcement training classes. Through my training and experience, I have developed an understanding of common habits and practices used by those engaged in criminal acts against children.

2. I am familiar with and have participated in a variety of investigative techniques including but not limited to: surveillance, interviewing of witnesses/suspects, and the execution of search and seizure warrants that involved child exploitation and/or child pornography offenses, and the search and seizure of computers and other digital devices.

PURPOSE OF AFFIDAVIT

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the following:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. The property located at 34 South 333rd Lane, Apt C, Federal Way, Washington 98003 (hereinafter the "SUBJECT PREMISES"), more fully described in Attachment A, which is attached and incorporated herein by reference.

b. The person of MICHAEL MORRILL, YEAR OF BIRTH: 1972, SOCIAL SECURITY NUMBER: XXX-XX-2997 (hereinafter the "SUBJECT PERSON"), more fully described in Attachment A, which is attached and incorporated herein by reference.

c. A 2019 Kia Forte (WA License BNK5436) (hereinafter the "SUBJECT VEHICLE"), more fully described in Attachment A, which is attached and incorporated herein by reference.

4. As set forth below, there is probable cause to believe that the SUBJECT PREMISES, SUBJECT VEHICLE, and SUBJECT PERSON will contain or possess evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography), as well as attempt or conspiracy to commit such offenses (hereinafter the "TARGET OFFENSES"). I seek authorization to search and seize the items specified in Attachment B, which is incorporated herein by reference.

5. The information in this affidavit is based upon the investigation I have conducted in this case, my conversations with other law enforcement officers who have engaged in various aspects of this investigation, and my review of reports written by other law enforcement officers involved in this investigation. Because this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are sufficient to establish probable cause to support the issuance of the requested warrants. When the statements of others are set forth in this affidavit, they are set forth in substance and in part.

6. This Affidavit is being presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUMMARY OF THE INVESTIGATION

7. This investigation involves a target who, acting via the online alias "[redacted] has participated in and/or distributed child pornography via websites that operate on the Tor anonymity network that facilitate the advertising and distribution of child pornography. The investigation identified evidence that an e-mail account through which the target communicated was accessed from the TACOMA PREMISES, a previous address of the SUBJECT PERSON who now resides at the SUBJECT PREMISES in Federal way. Further investigation revealed that images, including sexually explicit images, that were distributed online by [redacted] and via another online alias appear to depict an identified minor child who is related to the SUBJECT PERSON.

Background on the Tor Network

8. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

9. The websites further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org. The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network. A user may also access and use the Tor network through any computer or electronic device that has been configured to use Tor routing/software, to include desktop or laptop computers, smartphones, or tablet computers.

11. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

12. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the contents of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

13. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

14. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

15. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dflku7f" or "asdlk8fs9dflku7fasdlk8fs9dflku7fasdlk8fs9dflku7fasdlk8fs," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address—and therefore the location—of a computer server that hosts a hidden service.

Participation of [redacted] on Tor Websites A, B and C

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

16. As set forth below, there is evidence that a user with the alias "[redacted]" was an active member of Websites described herein as A, B, and C, all of which operate or operated as hidden service websites on the Tor anonymity network.[1] [redacted] Based upon my training and experience and the investigation as described herein, I believe that user [redacted] on Websites A, B and C to be the same individual.

Website A

17. WEBSITE A was an online chat website, the stated purpose of which was to be a chatroom dedicated to discussion related to girls between ages six to sixteen, that operated from approximately [redacted] It allowed users to engage in online chat with other users, either within chat rooms that were openly accessible to any user of the site, within rooms only accessible to particular users, or in one-to-one chats between two users. Website A users routinely advertised and distributed child pornography through Website A by posting web links within chat messages. These links allowed other Website A users to navigate to another website, such as a file-hosting website, where images and/or videos of child pornography were stored in order to download these image

[1] The actual names of Websites A, B and C are known to law enforcement. Investigation into the users of the sites remains ongoing and disclosure of the names of the sites would potentially alert other targets of the investigation, potentially provoking them to notify other users of law enforcement action, flee, and/or destroy evidence.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and videos. Website A provided its users with information about particular file hosting websites where users could upload digital files so that the files could then be shared, via links, with other Website A users. FBI Special Agents accessed and downloaded child pornography files distributed via Website A while it operated.

18. [redacted] After registering a user account on Website A, a user had to log in to that user account with the appropriate user-generated password in order to communicate via that user account on Website A.

Website B

19. WEBSITE B is another online chat website that is currently operating and facilitates the advertisement and distribution of child pornography. Similar to Website A, Website B allows users to engage in online chat with other users, either within chat rooms that are openly accessible to any user of the site, within rooms only accessible to particular users, or in one-to-one chats between two users. Website B users routinely advertise and distribute child pornography through Website B by posting web links within chat messages. These links allow other Website B users to navigate to another website, such as a file-hosting website, where images and/or videos of child pornography are stored in order to download these images and videos. Website B provides its users with information about particular file hosting websites where users can upload digital files so that the files can then be shared, via links, with other Website B users. Entry to Website B is obtained through free registration. FBI Special Agents have accessed and downloaded child pornography files distributed via Website B.

Website C

20. WEBSITE C is an online bulletin board that is currently operating and facilitates the advertisement and distribution of child pornography. Entry to the site is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

gained through free registration. After agreeing to the board rules, the user creates a username and password. No other information is required to register. Upon gaining entry, the user is presented with several categories of material including [redacted]

21. The "Rules" section has a single forum. Inside the forum are two topics, one of which is the "Board Rules." The first rule states [redacted]

22. In the "Contents" section are forums for "Nonnude," "Softcore," "Hardcore," "Teens," "Live Streams," "Fetish," "Naturist," "Art," "Literature," and "Requests." There are 573 topics and 2.832 posts under "Hardcore," which is the most of any forum. Under the "Hardcore" forum are categories for images and videos. Under the images category are topics including [redacted] FBI Special Agents have accessed and downloaded child pornography from Website C.

FBI Undercover Investigation of [redacted]

23. On April 19, 2020, an FBI undercover agent entered Website A and engaged user "[redacted]" in private message chat. During the conversation, the FBI undercover asked [redacted], "are you same from [Website C]? i remember the spelling lol." [redacted] responded, *"Yup, that is me. I keep the same nic so people can recognize me. It is the same reason I mis-spell [redacted]."* I am aware from training and experience that the term "nic" is shorthand for "nickname."

24. On April 22, 2020, an FBI undercover agent entered Website A and engaged user "[redacted]" in private message chat. During the conversation, "[redacted]" shared a digital file with the FBI undercover agent and stated, "*not for public posting please!*" The FBI undercover agent viewed and downloaded the file, which consisted of a digital image. The title of the file was "[redacted]" The image depicted a girl who appeared to be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

approximately [redacted]

25. On June 27, 2020, an FBI undercover agent entered Website A and observed that user "[redacted]" had posted a message in the open chatroom on Website A, "[redacted]," followed by links to the following images:

- An image depicting a fully nude girl [redacted]
- An image depicting a fully nude girl [redacted][3]

26. Following these posts, user "[redacted]" posted the following message in the same chatroom: "[redacted]"

I am aware from training and experience that "[redacted]" is shorthand for "[redacted]," i.e., the type of sexual object depicted in one of the images.

---

[2] Estimates of the approximate age of children depicted in the files described herein are based upon general life experience, personal interactions with children of all ages in personal and professional settings, including with victims of child exploitation offenses, prior viewing of images depicting the sexual exploitation of children, and my training and experience as a law enforcement agent.

[3] These images are available for review by the issuing magistrate upon request.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Investigation of Further Message Postings by "[redacted]"

27. [redacted] An analysis of the [redacted] postings made by "[redacted]" to those websites reveals evidence that "[redacted]" has a sexual interest in children and has engaged in activity related to child exploitation and pornography (all grammar and spelling as in original).

28. On or about [redacted] 2020, "[redacted]" posted on Website C: "[redacted]"

29. On or about [redacted] 2020, "[redacted]" posted on Website C: "[redacted]."

30. On or about [redacted] 2020, "[redacted]" posted on Website A: "[redacted]"

31. On or about [redacted] 2020, "[redacted]" posted on Website B: "[redacted]" I am aware from training and experience that [redacted].

32. On or about [redacted] 2020, "[redacted]" posted on Website B: "[redacted]\"

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

33. On or about [redacted], 2019, "[redacted]" posted on Website C: "[redacted]"

34. On or about [redacted] 2019, "[redacted]" posted on Website B: [redacted]

35. On or about [redacted] 2019, "[redacted]" posted on Website B: [redacted]

Investigation of E-Mail Account Associated with [redacted]

36. On or about June 27, 2020, an FBI undercover agent engaged "[redacted]" in a private message communication on Website A. During that conversation, "[redacted]" asked the FBI undercover agent whether the agent had an email account on [redacted], a Tor-network-based email service. [redacted] then provided the FBI undercover agent with the Tor network web address in order for the FBI agent to create an account on that e-mail service. "[redacted]" also stated, "I have one listed as [redacted]." The FBI undercover created an account on that e-mail service and shared the account address with "[redacted]" via a private message on Website A. [redacted] then replied to the FBI undercover agent, "check your new mail address. Sent you a test mail." Between June and October 2020, the FBI undercover exchanged multiple emails with "[redacted]" at the [redacted] address. During those emails, "[redacted]" referred to a girl as "[redacted]" who he had previously claimed was his [redacted] in private messages to undercover FBI agents on Website A. In one communication dated October 6, 2020, "[redacted]" stated, "Not much on the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

sexual front between me and [redacted]. No pics or videos [redacted] As described herein, [redacted] has distributed an image of a young girl with the name "[redacted]" in the filename.

Evidence Identifying a Premises Associated With "[redacted]"

37. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the site(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the site is located or the offender appears to reside, in accordance with each country's laws. I am likewise aware that U.S. and foreign law enforcement agencies investigate images distributed via websites including Tor hidden service websites such as those described herein in an effort to identify not only offenders associated with those images, but also children who are depicted in the images.

38. [redacted]

39. [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

40. [redacted]

INFORMATION REGARDING THE TACOMA PREMISES

41. According to publicly available information, IP address 76.28.167.60 is owned by Comcast Communications. On October 13, 2020, an emergency subpoena request was issued to Comcast Communications for information related to IP address 76.28.167.60 on October 7, 2020, at 00:26:37 UTC. Comcast Communications produced records showing that the IP address 76.28.167.60 was assigned to the TACOMA PREMISES on October 7, 2020, at 00:26:37 UTC. Comcast Communications also provided the following related to subscriber information:

AccountNumber: 8498350080007066

Account Address: 5006 Varco Road NE, Tacoma, Washington 98422

Associated Customer Name: Chris Morrill

Contact Numbers: (253) 927-9013

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Email account: cmorrill6@comcast.net

42. [redacted]

43. A review of publicly available records listed the following possible residents of the TACOMA PREMISES:

[redacted], YEAR OF BIRTH: 1944, SOCIAL SECURITY NUMBER: XXX-XX-947

[redacted], YEAR OF BIRTH: 1947, SOCIAL SECURITY NUMBER: XXX-XX-9833

MICHAEL MORRILL, YEAR OF BIRTH: 1972, SOCIAL SECURITY NUMBER: XXX-XX-2997 (the SUBJECT PERSON)

[redacted], YEAR OF BIRTH: 1971, SOCIAL SECURITY NUMBER: XXX-XX-8622

OPEN SOURCE INVESTIGATION AND VICTIM IDENTIFICATION

44. [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

45. [redacted]

46. [redacted].

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

47. [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

48. [redacted]

[redacted]

49.

50. [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

[redacted]

[4] I am aware from training and experience that "[redacted]" was a user and administrator of a Tor network website dedicated to child sexual exploitation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

[redacted]

52. [redacted]

53. [redacted]

[redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

[redacted]

[redacted].

54. [redacted].

[redacted]

55. [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

56.

57.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

58. [redacted]

59. [redacted]

60. [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

61. As noted above, [redacted]'s [redacted] said the SUBJECT PERSON had moved to a new within the last few weeks. She could not recall the specific address, but when shown a Google Maps photo of the area identified the Glen Park at West Campus Apartments as the complex into which the SUBJECT PERSON recently moved. This unit is a townhome within the Glen Park at West Campus Apartments in Federal Way, Washington. Based on a conversation with the manager of the Glen Park at West Campus Apartments, it appears this address was the SUBJECT PERSON's prior Federal Way address. That representative reported that he moved out of Unit 14A1 in April and provided the TACOMA PREMISES as a forwarding address.

62. Law enforcmenet officers spoke with [redacted] by telephone on the afternoon of November 2, 2020. He reported that the SUBJECT PERSON had been living at the TACOMA PREMISES but recently relocated to 34 South 333rd Lane, Apt C, Federal Way, Washington 98003.

63. Washington DOL records show that the SUBJECT PERSON has a 2019 Kia Forte (WA License BNK5436) registered to his name at the SUBJECT PREMISES. Law enforcement officers also spoke with the SUBJECT PERSON by phone. He confirmed he lives at the SUBJECT PREMISES and that another adult relative shares that residence.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

64. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other

65. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Importantly, e-mail and cloud storage can be a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

66. Even if such individuals use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in their home, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

67. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

68. Given the above-stated facts, and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the SUBJECT PERSON is the person using the alias "[redacted]" and given the activities of that user, likely has a sexualized interest in children and depictions of children and that evidence of the TARGET OFFENSES is likely to be found at the SUBJECT PREMISES, on the SUBJECT PERSON, or in the SUBJECT VHICLE.

FRUITS, EVIDENCE, AND INSTRUMENTALITIES INSIDE THE SUBJECT PREMISES AND ANY CLOSED CONTAINERS AND ELECTRONIC DEVICES FOUND THEREIN

69. As described above and in Attachment B, this application seeks permission to search for and seize items listed in Attachment B that might be found in the SUBJECT PREMISES, on the SUBJECT PERSON, or in the SUBJECT VHICLE, in whatever form they are found. One form in which evidence, fruits, or instrumentalities might be found is data stored on a computer's hard drive or other digital device[5] or electronic storage media.[6] Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

70. Through my training and experience, and the information learned during the course of this investigation, I know that individuals who engage in child pornography

---

[5] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[6] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

offenses often keep physical evidence, fruits, and instrumentalities of their crimes inside their residences, including but not limited to, digital devices

71. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensic examiners, and my training and experience, I submit that if a digital device or other electronic storage medium is found in the SUBJECT PREMISES, on the SUBJECT PERSON, or in the SUBJECT VHICLE, there is probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be stored on those digital devices or other electronic storage media. As noted above, the investigation has shown, among other things that user [redacted] disseminated child pornography and erotica depicting a particular minor child, and that [redacted] has been associated with the SUBJECT PREMISES. There is, therefore, probable cause to believe that evidence, fruits, and instrumentalities, of the crimes under investigation exist and will be found on digital devices or other electronic storage media at the SUBJECT PREMISES, SUBJECT VEHICLE, and SUBJECT PERSON for at least the following reasons:

a. Based my knowledge, training, and experience, I know that computer files or remnants of such files may be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, this information can sometimes be recovered months or years later with forensics tools. This is because when a person "deletes" a file on a computer, the data contained in the files does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in "swap" or "recovery" files.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer has been used, what is has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Digital storage devices may also be large in capacity, but small in physical size. Because those who are in possession of such devices also tend to keep them on their persons, especially when they may contain evidence of a crime. Digital storage devices may be smaller than a postal stamp in size, and thus they may easily be hidden in a person's pocket.

72. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on digital devices found in the SUBJECT PREMISES, on the SUBJECT PERSON, or in the SUBJECT VHICLE because:

a. Data on the digital storage medium or digital devices can provide evidence of a file that was once on the digital storage medium or digital devices but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

where, and how" of the criminal conduct under investigation, thus enabling the United States to further establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g. registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search of "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer activity associated with user accounts and electronic storage media that connected with the computer. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit the crime (e.g. Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper content, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing a user's intent.

f. I know that when an individual uses a computer to store, receive, or distribute child pornography, the individual's computer or digital device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer or digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer or digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer or digital device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of text discussions about the crime; and other records that indicate the nature of the offense.

73. *Necessity of seizing or copying entire computers or storage medium*. In most cases, a thorough search of a premises for information that might be stored on digital storage media or other digital devices often requires the seizure of the digital devices and digital storage media for later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic copy of the digital media's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

74. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all the necessary technical manuals and specialized equipment necessary to consult with computer personnel who have expertise in the type of computer, operating system, or software application being searched.

75. The analysis of computer systems and storage media often relies on rigorous procedures designed to maintain the integrity of the evidence and to recover "hidden," mislabeled, deceptively named, erased, compressed, encrypted or password-protected data, while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment such as a laboratory, is typically required to conduct such an analysis properly.

76. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impracticable to search for data during the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

execution of the physical search of the premises. The hard drives commonly included in desktop and laptop computers are capable of storing millions of pages of text.

77. A search of digital devices for evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents may recover evidence with carefully targeted searches to locate evidence without requirement of a manual search through unrelated materials that may be commingled with criminal evidence. Agents may be able to execute a "keyword" search that searches through the files stored in a digital device for special terms that appear only in the materials covered by the warrant. Or, agents may be able to locate the materials covered by looking for a particular directory or name. However, in other cases, such techniques may not yield the evidence described in the warrant. Individuals may mislabel or hide files and directories; encode communications to avoid using keywords; attempt to delete files to evade detection; or take other steps designed to hide information from law enforcement searches for information.

78. The search procedure of any digital device seized may include the following on-site techniques to seize the evidence authorized in Attachment B:

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or co-conspirators.

b. On-site copying and analysis of volatile memory, which is usually lost if a computer is powered down, and may contain information about how the computer is being used, by whom, when and may contain information about encryption, virtual machines, or stenography which will be lost if the computer is powered down.

c. On-site forensic imaging of any computers may be necessary for computers or devices that may be partially or fully encrypted in order to preserve unencrypted data that may, if not immediately imaged on-scene become encrypted and accordingly become unavailable for any examination.

79. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

80. Based on the information set forth herein, there is probable cause to search the above described SUBJECT PREMISES, SUBJECT VEHICLE, and SUBJECT PERSON, as further described in Attachment A, as well as on and in any digital device or other electronic storage media found therein or thereon, for evidence, fruits and instrumentalities, as further described in Attachment B, of the TARGET OFFENSES.

KELSEY M. MENDOZA, Complainant
Special Agent, FBI

The above-named agent provided a sworn statement attesting to the truth of the foregoing Affidavit submitted to me by reliable electronic means pursuant to Fed. R. Crim. Proc. 4.1(a) on this 2nd day of November, 2020.

DAVID W. CHRISTEL
United States Magistrate Judge

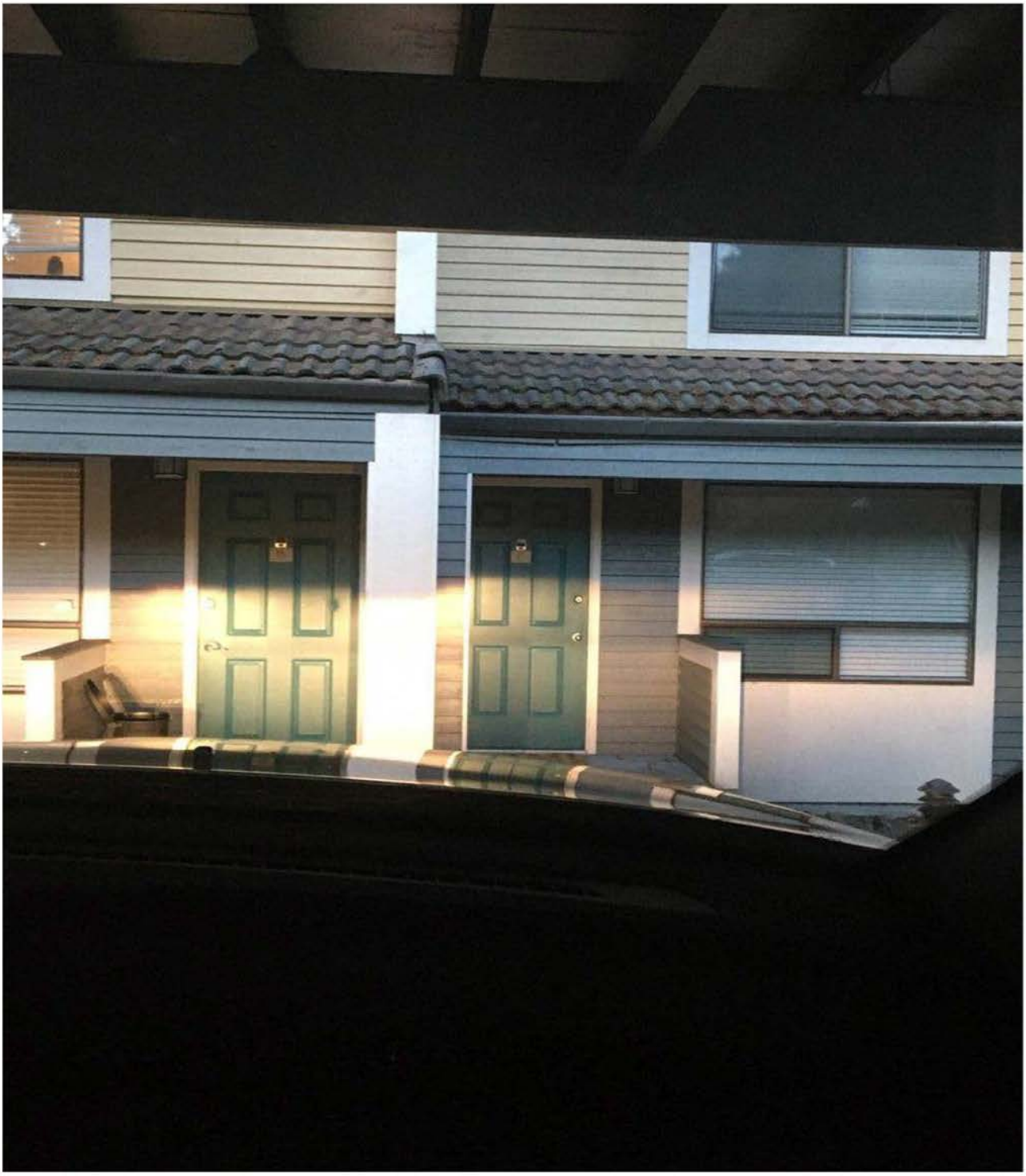
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Description of Property to be Searched

The physical address of the SUBJECT PREMISES is 34 South 333rd Lane, Apt C, Federal Way, Washington 98003, which is described as Apartment C, a unit within a multiunit building. The pictures below depict the SUBJECT PREMISES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



The search is to include all rooms within Apartment C and any storage areas or parking/garage spaces exclusively assigned to Apartment C, as well as any digital

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

device(s) or other electronic storage media found therein. However, if law enforcement can reasonably determine onsite that the SUBJECT PERSON neither owns nor has access to a particular digital device or electronic storage medium, this warrant does not authorize its search or seizure.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The SUBJECT PERSON is MICHAEL MORRILL, YEAR OF BIRTH: 1972, SOCIAL SECURITY NUMBER: XXX-XX-2997.

The search shall include the SUBJECT PERSON and any backpacks, bags, or other containers that SUBJECT PERSON may be carrying, and any digital devices(s) or other electronic storage media found.

The SUBJECT VEHICLE is a 2019 Kia Forte (WA License BNK5436). The search shall include the entire SUBJECT VEHICLE and any digital devices(s) or other electronic storage media found

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography), as well as attempt or conspiracy to commit such offenses committed in or after July 2016, as follows:

a. Items, records, or information[7] relating to visual depictions of minors engaged in sexually explicit conduct;

b. Items, records, or information relating to the identity of the creator(s) of or subject(s) depicted in any visual depiction of a minor engaged in sexually explicit conduct;

c. Items, records, or information relating to the location of or circumstances surrounding the creation of any visual depiction of a minor engaged in sexually explicit conduct;

d. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

e. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

f. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;

---

[7] As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Items, records, or information related to communications with or about minors;

h. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;

i. Items, records, or information concerning travel;

j. Items, records, or information concerning websites operating over the Tor network, including any document or page comprising a part of any such website, records and information showing any person's access to or involvement with such websites, and any communications between any users of such websites;

k. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, purchase or lease agreements, diaries, statements, identification documents, address books, telephone directories, and keys;

l. Items, records, or information concerning the ownership or use of computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for internet access, handwritten notes, and computer manuals;

m. Any digital devices or other electronic storage media[8] and/or their components including:

i. any digital device or other electronic storage media capable of being used to commit, further, or store evidence, fruits, or instrumentalities of the offenses listed above;

[8] The term "digital devices" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "electronic storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ii. any magnetic, electronic or optical storage device capable of storing data, including thumb drives, SD cards, or external hard drives;

iii. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

iv. any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

n. For any digital device or other electronic storage media whose seizure is otherwise authorized by this warrant, and any digital device or other electronic storage media that contains or in which is stored records or information that is otherwise called for by this warrant:

i. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

vi. evidence of the times the digital device or other electronic storage media was used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

vii. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

viii. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

ix. records of or information about the Internet Protocol used by the digital device or other electronic storage media;

x. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

xi. contextual information necessary to understand the evidence described in this attachment.

o. A dark colored blanket with purplish-pink pattern and border.
p. A purple anal sexual object

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970